

## Evaluation Scoring

### **Notes to Evaluators:**

Please provide detailed comments to assist in the consensus and debrief process.

**Suggested scoring valuation:** Please notice many of these points are not on a 1 to 5 scale and must be adjusted accordingly.

### **Remember to be consistent with scoring methodology**

#### **Example use only**

0	Did not provide an answer	Firm Experience	Staffing/Resumes	Sample
1	Incoherent, communicates a lack of understanding and/or capability	7	5	3
2	Marginal, communicates a weak knowledge, understanding, and/or capability	14	10	6
3	Average, communicates an average knowledge, understanding, and/or capability	21	15	9
4	Good, communicates that they are good at what they do and have a good understanding	28	20	12
5	Excellent, communicates that they are not just good, but provide value added services and capabilities that may exceed expectations	35	30	15

#### **Quotation Section (10%) Cost Proposal Score will be calculated by the contract manager.**

The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. This means that the overall score for the cost proposal will account for the robustness of the proposer's qualifications as well as their proposed price. We will include both the blended hourly rate and the price quote in scoring the cost proposal. The cost proposal will be worth up to 10 percent of the total possible points – see the table on page 26 of the RFQQ.

#### **Qualifications Section (65%)**

##### **Firm Experience (35%)**

The Qualifications Section of the proposal must contain information that will demonstrate to the evaluation committee the Firm/Staff understanding of the types of services proposed, the ability to accomplish them, and the ability to meet tight timeframes. Firm experience will be scored based on the capacity and experience of the firm to perform work similar to the tasks described in this RFQQ.

##### **Staff Experience/Resumes (30%)**

Staffing will be scored on how the proposer staffs the project to perform work similar to the tasks described in this RFQQ, including the number of staff and the mix or make of the team and their various levels of experience. see page 23 of the RFQQ for details. The proposer must provide a resume for key staff and include information on the individual's specific skills, experience, certifications, significant accomplishments and responsibilities assumed on other similar projects related to the services proposed.

#### **Sample Reports (15%)**

This sample report will be scored based on how well its components respond to items listed under item "e." under "Report Results" on page 4 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.

#### **Executive Order 18-03 & WA Small Business/Veteran Owned Business(10%) will be calculated by the contract manager.**

This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver.

K689 - Security Assessment Services			
Vendor: Accenture			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/10/23: Blended hourly rate of <b>\$255.00</b> is high. Total cost of the sample engagement seems high, but this is likely a function of the hourly rate.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Firm experience is extensive: over 20 years of experience in their Security Practice division; hundreds of security assessments conducted; claims to have one of the largest offensive security capabilities in the world with deep specialization; 300+ security testers. Lists mobile, webapp, IT infrastructure, cloud, and source code review as capabilities, <b>but does not explicitly list testing of mainframes, IOT devices, or ICS/SCADA as capabilities</b> . Customers include hundreds of Fortune 500 businesses, though this may be in non-pentest services. The listed callable references included penetration testing, but also more general risk and controls assessments, which are not what this RFQQ is requesting. Similarly, of the five listed representative projects, only 4 of them included penetration testing, and only 3 of them were pure penetration test engagements (as opposed to having penetration testing being just a part of the engagement). This undermines their responsiveness to the services requested in this RFQQ.  The total window of time dedicated to the sample pentesting engagement is high, with the test window itself spanning 7 weeks (not including scoping or any post-reporting activities, such as Q&A). <b>This appears to be a function of a relatively small team, with only two full-time pentesters assigned to the project, supplemented by two part-time SMEs for specific parts of the work.</b> Additionally, the project team and structure proposes the bidder's project leads as being in direct contact with the state agency contacts, with SAO's contact being further outside. This implies that the bidder plans to not work through SAO's designated audit leads and IT security specialists when planning or overseeing an engagement (the RFQQ states "The State Auditor's Office will collaborate with the contractor and state agencies or local governments to identify the networks, applications, operational technology and information systems to be included in the scope of testing for each state agency or local government."), but instead as the bidder outright directing the engagement.
Staffing (30%)	30.0	18.0	Bidder provides resumes for 10 employees, but of those, one is an executive (Michele Myauo) and a second is a high level manager (Mark Williams). Of the eight remaining resumes, only 4 (Thulani Shabangu, Rob Hettinger, Ian Nespolo, and Grant Buben) explicitly list penetration testing among their selected experiences, and one other (Greg Conover) lists penetration testing as an area of focus. Much of the cited areas of focus and experiences are either in areas that are not as thorough or specific as a penetration test (e.g., vulnerability scanning/analysis, security architecture, threat assessments, cloud migration), or are wholly unrelated to penetration testing (e.g., IT mergers and acquisitions).
Qualifications Section Total Score	65.0	39.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	Page 6 of Bidder's sample report includes an executive summary that is fairly technical. Page 7 lists the findings by their CVSS severity, the impact of those vulnerabilities, and their exploitability. The sample report included areas for improvement, but <b>did not</b> include overall statements of areas of strength. The detailed technical findings (beginning on pg. 9) list the description, impact, and recommendation for each finding. However, those portions are very brief, do not provide much context (i.e., how could a specific finding affect the organization's operations or ability to function), and generally only list one or two supporting sources (and occasionally none). Furthermore, the evidence (e.g., screenshots) are listed in a separate section of the report (beginning on pg. 32), which requires a reader to jump back-and-forth between the two sections in order to gain a complete understanding of the nature of the finding.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	45.0	
Evaluator Initials : JOC			
Date: 5/10/23			

Affinity IT			
K689 - Security Assessment Services			
Vendor: Affinity IT			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/10/23: Bidder's blended hourly rate of <b>\$171.25</b> is competitive. However, their total sample state agency cost of \$30,820 is unusually low (that type of dollar amount would typically be seen on a very small engagement). Reviewing the time estimates the bidder provided for each part of the work (pgs. 22-32 of the proposal), I estimated this would cost roughly \$35k (which is still very low). Specifically: Internal app 1: 3 days (approx. 24 hours) Internal app 2: 3 days (approx. 24 hours) ICS network: 5 days (approx. 40 hours) Firewall review: 2 days (approx. 16 hours) Network penetration testing: 3 days <b>assuming 500 IPs</b> , but the sample assumes >1000 IPs. Therefore, I assumed 6 days of work instead of 3 (approx. 48 hours) External website: 0.5 days (approx. 4 hours) External app 1: 3 days (approx. 24 hours) External app 2: 3 days (approx. 24 hours) Total estimated hours: 204. <del>Total estimated cost @ blended hourly rate: \$34,935</del>
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Bidder notes having over 13 years of experience in security. All three provided references included network penetration testing, two of them included web application security testing, ad one of them included wireless network testing. Sample proposal does decent job of outlining the project management steps for preparing for a pentest, but does not thoroughly discuss the manual techniques the test team would employ to test the in-scope assets. It also provided a proposal for a smaller network scope than what was explicitly listed in the sample. Of the five representative projects the bidder identified (pgs. 50-54), all five included network penetration testing, and one of them included wireless testing (Chicago Housing Authority), but only one (Lincoln Tech) explicitly listed web-application security testing, and the associated deliverable seems to have been a vulnerability report (which may mean that it did not include manual penetration testing techniques). The examples also included other lines of work that this RFQQ generally is not looking for, including physical penetration testing and more general security controls assessments. <b>Additionally, aside from including/responding to the RFQQ's prompts, the proposal does not explicitly mention experience conducting penetration tests of mobile applications, thick clients, mainframes, or operational technology.</b>
Staffing (30%)	30.0	18.0	Page 39 of the proposal states that the bidder has 10 staff, but of those, 4 are contractors (meaning full-time staff is 6). Additionally, of those 6 full-time staff, one is an office administration/operations manager, and another is a sales associate. On page 42, the bidder lists 6 proposed staff to work on this contract. However, this includes two that are identified on pg. 39 as contractors (Thomas Czerniecki and Brian MacPhee), and their resumes (pgs. 47-48) consist almost entirely of skills and experience that this RFQQ does not seek (e.g., municipal management, law enforcement, etc.). The resumes for the 4 identified staff with documented penetration test experience (Joseph Fisher, Konrad Gawronski, Michael McCormick, Daven Ryerson) don't provide many details about the types of systems they tested, or the sizes of the engagements they've worked on.
Qualifications Section Total Score	65.0	32.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	3.0	The bidder provided two sample reports: an external network report beginning on page 62, and an internal network report beginning on page 70. However, as evidenced by the formatting and verbiage of both reports (particularly the internal network report) and the omissions as described below, it is apparent that both reports are the result of automated vulnerability scans rather than true, thorough penetration tests.  The external report is very brief. While it says the scope included web-based applications, the scope (which was redacted for valid confidentiality reasons) is described as consisting of IP ranges rather than URLs, suggesting that web-based applications may not have actually been tested (i.e., the scope may have just been a network test). The number of results (4 total findings) further suggest this. While both reports include an executive summary, neither report includes a summary of strengths within the targeted organization, and only includes a brief summary of weaknesses. Additionally, neither report includes detailed remediation steps or a description of impact that includes any kind of meaningful context (i.e., beyond a technical description of the vulnerability). Neither report provides detailed testing methodologies or screenprints, nor do they describe the likelihood or difficulty of a particular vulnerability being exploited.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	35.0	
Evaluator Initials : JOC			
Date: 5/10/23			



K689 - Security Assessment Services			
Vendor: Berry Dunn			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/10/23: Bidder's blended hourly rate of <b>\$235.00</b> is high, but the cost for the sampled state agency (\$48,007.20) seems low.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Limited firm experience; bidder notes on page 3 that their firm has "been conducting vulnerability scanning and penetration testing for more than five years." As noted on pfs. 14-15, the bidder has conducted other work for 16 local governments and 4 state agencies in Washington state. However, none of it is penetration testing, and only a portion of it is related to IT. The bidder provided 3 references (pgs. 22-24), but only one of the engagements lists penetration testing (New Mexico Health Insurance Exchange), and it was only one part of a larger engagement. That engagement, along with the other two references, pertain more to reviewing and/or developing the clients' overall IT security and risk management programs, and reviewing controls and configurations for compliance requirements.  On pg. 33, the proposal describes deliverables that stray from what was requested in the RFQQ, stating "Our vulnerability and risk assessment will take a holistic approach that focuses on the people, processes, and technology to help develop a risk profile for each agency and local government that is tested. Where typical vulnerability scanning and penetration testing primarily focus on the technology, this proposed approach will provide the SAO and tested entities with a more complete understanding of the potential risks each agency, department, or system may face."  Bidder's description of penetration testing on pgs.34-35 is not very detailed. For example, it does not discuss whether the bidder would conduct authenticated testing, or what types of exploits it would attempt (e.g., code injection, cross-site scripting, malicious file upload, etc.).  Pages 43-44 list some of the platforms the bidder has conducted work on, indicating experience with testing cloud-hosted assets as well as mainframes. <b>One of the representative engagements also notes that a mainframe was included within the scope. However, aside from including verbiage from the RFQQ, the bidder does not mention testing of thick client or mobile applications, nor does the bidder mention testing of operational technology. There is one reference to SCADA testing on page 47, but this is described as a test of a production/business network to ensure that an attacker could not connect to a SCADA network.</b>  Of the five representative projects listed (pgs. 44-47), all five included penetration testing, though one (City of Scottsdale) appears to have only been wireless testing. All five engagements appear to have included penetration testing as only a portion of a larger engagement. The bidder listed additional projects on pgs. 47-48 that included penetration testing, but with fewer details.
Staffing (30%)	30.0	6.0	Bidder lists resumes for 4 individuals in the proposal (pgs. 51-65). Of these 4, one (Bill Brown) is a principal who would not be directly conducting any of the testing, and one (Matt Bria) is listed as a project manager, who would also likely not be directly conducting any testing. <b>Of the 2 remaining listed individuals, only one (Mitch Darrow) is listed as having extensive experience directly conducting penetration tests</b> ; the other individual (Louis Krupp) is a security analyst whose cited work consists of more general IT security experience, such as reviewing policies/procedures, analyzing scan results, and conducting controls assessments against compliance or security frameworks.
Qualifications Section Total Score	65.0	27.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	Bidder's sample report (pgs. 67-95 of the proposal) includes a very brief executive summary that includes some higher priority results, but does not provide an overall statement of strengths or opportunities for improvement. The overall structure of the report is built like a methodology, talking extensively about the steps the bidder took in this engagement. However, as a result, the test's findings are sorted in the order in which they were discovered, rather than in a more conventional and user-friendly way, such as by severity. The results themselves contain very little detail beyond the name of the finding, the affected system(s), and sometimes an assesement of their severity. Any discussion regarding the difficulty for an attacker to exploit the identified findings, recommendations to remediate them, and discussion of how those findings impact the affected systems is included in sections that come after the findings are themselves listed, which requires a reader to jump back-and-forth between the two sections in order to gain a complete understanding of the nature of the finding.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	33.0	
Evaluator Initials : JOC			
Date: 5/10/23			

BPM			
K689 - Security Assessment Services			
Vendor: BPM			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/10/23: Blended hourly rate of <b>\$195.00</b> is reasonable, and the overall estimated cost of the sample engagement (\$79,800) is within the ballpark of similarly-sized engagements. <b>The bidder's quotations section (Exhibit C) does not contain any further details on how the bidder would approach the sampled scope of work, such as the project approach/methodology, a workplan, a project schedule, or deliverables.</b>
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Bidder's references (listed on pg. 4 of Exhibit A-2) lists five government organizations, all of which had penetration testing conducted, ranging from network and web application penetration testing to a SCADA (ICS) assessment. These are also listed in Exhibit D as representative projects (pgs. 3-5), but feature few additional details about the number of applications/systems tested. While two of these included SCADA systems, none of the referenced work discusses testing performed on thick clients, mainframes, or mobile applications.  Page 6 of Exhibit D briefly discusses the bidder's history, noting that the bidder has performed over 1,200 comprehensive penetration tests and over 600 information security program reviews, configuration reviews, and risk assessments. However, it also does not provide many additional details, such as types of systems tested, industries covered, or anything regarding their penetration testing methodology. Page 7 includes a paragraph about continued work with government organizations in the state of Oregon.
Staffing (30%)	30.0	12.0	Bidder lists resumes for 10 staff (pgs. 9-11 of Exhibit D), however nearly all of these staff do not have their last name listed, and all have very brief resumes, providing little detail on actual projects they have completed. Of the 10 staff listed, only 3 (David T., Sam Z., Jon P.) list extensive penetration testing experience; the experience listed for the remaining staff fall in other areas of IT and IT security, or in project management.
Qualifications Section Total Score	65.0	33.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder's sample report includes an executive summary that lists strengths and areas of opportunity. However, it also states "Once these remediation efforts have been completed, FICTITIOUS ORGANIZATION will have a strong security posture," which is an assurance that goes beyond what a typical penetration test should provide (e.g., there are many factors that affect an organization's security posture that will fall outside the scope of most penetration tests, such as excessive privileges, employee behavior, vendor contracts, and incident response capabilities, to name a few). The detailed results are grouped based on the type of work performed; at the introduction of each type, the sample report includes a thorough description of the types of assets tested, why they should be secured, and what the impact of a compromise could be. The results themselves are concise and include remediation steps, evidence, and additional technical references. Each result also includes a risk rating, however the calculus that goes into this (Severity vs. Likelihood/difficult) is not clear.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	42.0	
Evaluator Initials : JOC			
Date: 5/10/23			

K689 - Security Assessment Services			
Vendor: CAI			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.
			JOC 5/11/23: Hourly rate of <b>\$144</b> is very competitive, and total cost of sample agency assessment (\$81,072) is also within the range expected for an engagement of that scope and size. The workplan the bidder provided (Exhibit C, pg. 4) shows clear timelines. However, the overall timeframe estimated (6 weeks of actual testing) is a bit longer than we would expect for an engagement of this size, which could present issues considering how many engagements our audits conduct every year. The bidder adeptly acknowledges on pg. 5 of Exhibit C that the scoping phase takes place over a number of weeks, thereby effectively caveating the proposed timeline for scoping as shown in the workplan.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Bidder states on pg. 2 of Exhibit D (Qualifications) that they have experience testing web and mobile applications, as well as operational technology/ICS (pg. 4), <b>but aside from including/responding to the RFQQ's sample state agency scope, the bidder does not discuss any experience conducting penetration testing of thick clients or mainframes.</b> Bidder's methodology, as described on pgs. 6-10, is well described, particularly in terms of the considerations for scoping and logistics of an engagement. It proposes a very collaborative approach, which is ideal. Bidder has extensive experience working with government, but all of its government clients appear to have smaller contracts than what this contract would entail (pg. 11); this suggests that either the bidder's government work has been mostly in non-penetration test services, or their penetration testing at those government clients has been minimal.  Of the bidder's 5 representative projects (Exhibit D pgs. 12-15), only four included penetration testing. (However, the cited project that did not, Metropolitan Water District of Southern California, resulted in discovery of a live threat actor within the client's environment). Of the four projects that included penetration testing, none are listed as having included application testing; however, one (Metra Rail) did include testing on OT/SCADA assets.
Staffing (30%)	30.0	6.0	The bidder provides resumes for only three individuals on pgs. 19-24 of Exhibit D, with summary bios of them on pg. 17. Of these three individuals, one (Rex Johnson) is an executive director of the firm's cybersecurity division, one (Pedro Ortega) appears to be a senior penetration tester, and one (Annie Liao) appears to be a junior penetration tester. The resume for Pedro Ortega does not specify timelines for his prior employers, making it difficult to gauge how many years of penetration test experience he has (he has only been with the bidder since 2021). The timelines listed in the resume for Annie Liao indicate that her penetration testing experience only extends as far as her tenure with the bidder (beginning in 2022).
Qualifications Section Total Score	65.0	27.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	Bidder's sample report includes an executive summary with summary statistics and mid-level details of their findings (e.g., areas for improvement), but it does not identify areas of strength. The detailed results do include a risk level, based on CVSS scoring, but the description of each result is very brief, and therefore lacks context around what these individual results can mean for the organization's functions (i.e., factoring in how the affected assets support the organization). The results also do not articulate the likelihood or difficulty of each result being exploited. The solutions (recommendations) are also very brief, and the report does not include references where the recipient can find additional information. Furthermore, evidence (e.g., screenshots) is listed in the pages below the table of results, requiring a reader to jump back-and-forth in order to gain a more complete understanding of how to identify a given result. The scope of the engagement in the sample report appears to be heavily focused on network testing, therefore providing a very limited representation the types of application testing findings that the bidder would report on.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	33.0	
Evaluator Initials : JOC			
Date: 5/11/23			



K689 - Security Assessment Services			
Vendor: Deloitte			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/11/23: Bidder's hourly rate of <b>\$149</b> is very competitive, but their proposed project cost for the sampled agency ( <b>\$118,993</b> ) is higher than expected given the scope of testing.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	28.0	In Exhibit A-1, Bidder lists ongoing/prior work with three Washington sate agencies, some of which might overlap with the scope of assets that would be included in a penetration test. On pg. 5 of Exhibit C, bidder lists a few additional government organizations they have provided services for in Washington, but does not specify in detail what those servers were. One of the few details the bidder does mention here is that "we have experience integrating with SecureAccess Washington® (SAW/SEAP)." <b>Since many applications at the state agencies we have audited authenticate through SAW/SEAP, this could present an indepence or conflict of interest issue.</b>  Bidder uses ambiguous language to describe the extent of their penetration test experiencing, stating on pg. 4 of Exhibit C: "Over the past decade alone, we have performed over one thousand Cybersecurity engagements, including numerous Penetration Testing Assessments."  Bidder describes their methodology with good detail on pg. 10-21 of Exhibit C. However, they note in step 5 on pg. 10 that data exfiltration is part of their approach. <b>Data exfiltration is generally not part of SAO's penetration tests beyond what is needed to demonstrate proof of concept. Including this step as part of the approach can cause SAO to incur additional reputational risk and legal liability considering the types of data that are regularly used by the organizations SAO audits.</b> Bidder states on pg. 11 that mainframe testing is within their capabilities. <b>On pg. 12, bidder says "Deloitte will conduct white box (no harm) testing activities on the in-scope web applications." However, penetration testing always carries some level of risk, particularly if conducted in production environments (and not all agencies and local governments have non-production environments available for testing). Therefore, this comes across as an unrealistic/overly optimistic assumption.</b>  The aforementioned methodology discussed familiarity testing web applications, mainframes, mobile applications, and OT/SCADA. <b>However, it doesn't explicitly note familiarity testing thick client applications.</b> Page 13 lists "custom apps" as an area that the Bidder is prepared to conduct penetration testing, but under the steps for that area it includes "Gather ... web pages," which suggests that this are may just be in reference to custom-built web applications.  Bidder provides five representative projects on pgs. 3-6 of Exhibit D. Of these five projects, at least 4 included manual penetration testing, while the fifth (Oregon Health Authority) is described in a way that suggests the test was limited to automated scanning and techniques (i.e., not a full penetration test).
Staffing (30%)	30.0	24.0	Bidder provides resumes for 13 individuals (Exhibit D pgs. 9-21). Of the four individuals (Ian Fleming, Keith Howell, Olu Afolabi, Albert Tao) that are listed as Key Personnel on pg. 7, 3 (Keith Howell, Olu Afolabi, Albert Tao) have direct experience conducting penetration tests according to their resumes. The remaining 9 individuals are not listed as Key Personnel on pg. 7, but are listed as proposed penetration testers in their resumes. Eight of these 9 (David Caviness, Garrett Smith, Jed Anderson, Christopher Boedicker, Ricky Lak, Ayesha Rizvi, Neel Patel, Victor Falade) have varying levels of experience conducting penetration tests, either in the form of hands-on experience or experience working in a support capacity. While this indicates a deep bench of penetration testers, <b>the resumes did not specify in detail whether or not these individuals had experience testing thick client applications or mainframes</b> (one resume mentioned testing mobile applications, and another mentioned <i>maintaining</i> operational technology systems).
Qualifications Section Total Score	65.0	52.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	Bidder provided a rather brief sample report (pgs. 22-36 of Exhibit D), but it only appears to be of a network penetration test, and does not articulate much work performed as part of application penetration testing. The report includes an executive summary with some conclusions, including a summary of areas for opportunity. But it does not discuss areas of strength. The sample report only provided one detailed findings (pg. 30), making it difficult to gauge how different types of findings (e.g., more simple results vs. more complex results) would be presented. <b>While the one finding that was provided did include a moderate description of the result, a description of the impact that is contextualized to the environment, recommendations, and external references, it did not provide screenshots or other forms of evidence to allow the recipient to see/validate the result. Furthermore, the result was given a simple severity rating based on CVSS, but the likelihood/difficulty of the vulnerability being exploited was not provided.</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	58.0	
Evaluator Initials : JOC			
Date: 5/11/23 - 5/12/23			

K689 - Security Assessment Services			
Vendor: Digitech			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.
			JOC 5/12/23: <b>Serious concern here.</b> Page 1 of Exhibit A-1 says the bidder (LaSai Technologies, LLC (DBA Digitech Labs)) <b>has not</b> done business under any other name, and bidder attests on page 6 of Exhibit A-1 that they will <b>not</b> use sub-contractors. However, bidder provided multiple documents for "Strobes Security." On pg. 1 of Exhibit A-2, bidder clarifies this, stating that Strobes Security, Inc. is its "partner ... to deliver on this RFP scope of work." Therefore, bidder intends to use Strobes Security as a subcontractor, despite attesting in Exhibit A-1 that it would use no such sub-contractors. On pg. 3 of Exhibit A-2, bidder explicitly rejects the question about the sub-contractor, stating they have "a seamless, robust process that helps Digitech [bidder] to draw a combined team of best resources to deliver on this RFP scope of work." However, the way this is phrased means that Digitech will make contract decisions on behalf of Digitech and Strobes, while Strobes will only provide resources as determined to be necessary by Digitech. Therefore, Strobes would be functioning as a sub-contractor for this engagement.  Bidder's blended hourly rate ( <b>\$143.00</b> ) is very competitive, and the cost of the sample engagement ( <b>\$99,500</b> ) is within an expected range for this scope of work.  <b>Additional concern:</b> Bidder submitted what appears to be a separate proposal produced directly by Strobes ("Strobes - Security Assessment_DigitechLabs"). The content in this document appears to have been used to formulate the bidder's proposal (which is acceptable if declared as Strobes' content or if bidder received Strobes' permission to re-use it). <b>as well as additional pricing information near the bottom of the proposal.</b> This pricing breaks down the cost of tasks performed to be between \$90 and \$140 per hour, <b>meaning that the bidder's proposed blended hourly rate is between \$3 and \$50 more per hour than Strobes</b> (who, by nature of their proposal's detail, appears to be the party that would actually be doing the penetration testing work). In my judgement, this undermines the value of the bidder's blended hourly rate, as the bidder's surcharge may end up being solely for contract management rather than performance of actual penetration testing work. Additionally, since Exhibit C explicitly states "Proposers must provide a single, not-to-exceed, "blended hourly rate" price quote for the contract term " the inclusion of this information may undermine the bidder's responsiveness to the RFQO.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Bidder's work plan for the sample project (Exhibit C, pg. 2) adeptly outlines key pre-requisites for conducting testing, such as URLs, test credentials, and remote access to the internal network. The project schedule appears reasonable resourced in terms of the number of staff they would provide the engagement. But it breaks the project into smaller chunks - each with their own timeline - and some of those chunks inherently overlap (e.g., reconnaissance and OSINT), causing the overall timeline of the engagement to be a bit ambiguous.  Bidder states that their "specialist partner, Strobes security has 6+ years of dedicated, niche experience in delivering high quality vulnerability assessments that includes web applications, thick client applications, mainframes, operational technology, network and source code review" (Exhibit D, pg. 1-2). <b>While this acknowledges experience with the types of systems we expect the vendor to have experience with, this experience lies with a 3rd party/sub-contractor and is not very extensive ("6+" years).</b> (Bidder later asserts on pg. 2 that this experience includes penetration testing).  Bidder provides five representative projects on pgs. 3-5 of Exhibit D. Of these five, all included penetration testing of network segments and applications, and collectively, this included work on web applications, thick clients, mobile applications, and ICS/SCADA. <b>However, none of the cited projects included testing on mainframes. More glaringly, though, is that it is unclear if this work was performed by the bidder (Digitech) or by their "partner" (Strobes Security).</b>  Bidder provides a relatively detailed methodology (pgs. 7-14 of Exhibit D), but as with the representative projects, the bidder does not specify if this methodology is crafted by the bidder or their "partner." (Based on reviewing another document provided by the Bidder, "Strobes - Security Assessment_DigitechLabs," it appears that the Bidder used content from a proposal supplied by Strobes and presented it as their own for the purposes of this response). Bidder also lists prototypical human resources that would be provided to a project, consisting of a Consultant, a Sr. Security Analyst, and a Security Analyst. However, the latter two each have no more than 6 years of experience, while the Consultant is described as having "6+" years. Collectively, this indicates a relatively limited background among the human resources, which may be a limiting factor when testing systems that rely on older technologies (e.g., mainframes).
			Bidder provides resumes for four individuals (separate attachments), they are on Digitech Labs letterhead, and they do not mention "Strobes" at all. This indicates they are being represented as Digitech employees rather than Strobes employees. Of these four, three (Vatsal Agrawal, Prakash Ashok, and Shiva Krishna) have penetration testing experience, while the fourth (Bhushan Shinde) is a compliance manager with no listed penetration testing experience. <b>However, the three penetration testers are described as having approximately 4 years each of overall cybersecurity, with penetration testing activities constituting just a portion of that time.</b> All three penetration testers have experience testing web and mobile applications, and one of the individuals (Prakash Ashok) has experience with testing thick clients. <b>However, none have any listed experience testing mainframes or operational technology/ICS/SCADA.</b>
Staffing (30%)	30.0	18.0	
Qualifications Section Total Score	65.0	39.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder provided two sample reports instead of just one, but both of these were produced by Strobes, and not by Digitech. The Mobile sample report has an executive summary that lists the results at a summary level, but does not provide areas of strength. The detailed results include thorough descriptions that explain the vulnerabilities and why they're meaningful, both from a technical standpoint and within the context of the tested asset. The results also include screenshots, as well as steps to reproduce the result, allowing the recipient to understand how to validate the result for themselves, as well as mitigation steps. <b>However, the results contain few additional references (e.g., vendor websites, wikis), nor do the results rate the difficulty or likelihood of each vulnerability being exploited beyond just assigning a general severity rating.</b> The provided Network penetration test sample report was generally similar in nature, but with slightly fewer steps written out to reproduce the identified findings.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	48.0	
Evaluator Initials : JOC			
Date: 5/12/23			



EideBailly			
K689 - Security Assessment Services			
Vendor: EideBailly			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/15/23: Blended hourly rate of <b>\$175</b> is competitive, but their proposed sample agency cost <b>(\$48,125)</b> is low. However, the proposed timeline is within the range that would be expected of an engagement this size..
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Bidder's proposal is poorly written/tailored in a few areas. For example, the "Assistance from Your Staff" portion (pg. 9 of proposal) refers to holding meetings with "accounting personnel" and later says "We ask our clients to have the ... financial statements prepared by the requested dates." It also says "During the engagement, our use of SAO personnel will include answering questions, updating schedules, addressing issues identified and obtaining supporting documentation." This sentence either suggests that bidder intends to outright lead all phases of the penetration testing engagement with SAO as a minor participant (which is not acceptable; SAO oversees the project start to finish), or it suggests that SAO is the entity that is going to be tested (which is not accurate). All of this language is surely a carry-over from other proposals the bidder has submitted, but its inclusion raises concerns about the bidder's attention to detail and the care with which they produce their deliverables.  In general, the bidder's proposal is very generic, with relatively little of the content dedicated towards discussing their penetration testing experience, and a disproportionate amount of content dedicated towards discussing bidder's other consulting services and experience. The most the bidder says about their firm's overall experience conducting penetration testing is on pg. 29, where the bidder states "The seasoned professionals that provide cybersecurity and risk advisory services bring years of relevant technology experience, many of whom carry a myriad of relevant technical certifications, including the following designations." Bidder then lists the certifications that their cybersecurity staff possess (pgs. 36-37), but none of these are specific or even inclined towards penetration testing. Some are very generic (CISA, GSEC, CISM, CISSP) while others are in niche areas that are not penetration testing (GCIH, GCFE).  Bidder does list experience conducting testing on web applications, thick clients, mobile applications, and industrial control systems, <b>but does not mention any experience testing mainframes. Additionally, the bidder's proposed approach for describing testing on industrial control systems ignores what SAO stated in the pre-proposal conference, which is that many organizations do not have test environments of their industrial controls systems.</b>  Bidder lists five representative projects (pgs. 44-45), but describes them with such little detail that it's difficult to ascertain the size of the penetration testing engagements. Some of the engagements state that web application testing was included, but none describe <del>testing on other types of assets (e.g. thick clients, mobile applications, mainframes, industrial control svstems).</del>
Staffing (30%)	30.0	6.0	Bidder lists four individuals in the resumes section (pgs. 38-41). Of those four, (Kyle Hendrickson, Anders Erickson, Dale Lozo, Rob Else), <b>none</b> had experience conducting penetration testing listed in their resumes. Resumes for penetration testers were not provided, making it difficult to gauge the bidder's actual experience conducting penetration test engagements.
Qualifications Section Total Score	65.0	20.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	Bidder provided three sample reports (instead of one, as requested in the RFQQ). The first report (beginning on pg. 100) is an internal vulnerability assessment, which includes an executive summary and some summary-level results (findings and severity levels). But it does not include areas of strength. The detailed results provide a severity level, but this appears to be based on CVSS, and <b>does not further define the likelihood or difficulty of the findings being exploited</b> . The results include descriptions, supporting evidence (screenshots), solutions (recommendations) and links to external references, <b>but they are very brief, providing little context into how each of the vulnerabilities could be exploited</b> . The bidder's external penetration test report (beginning on pg. 128) and web application assessment report (beginning on pg. 147) were similar in nature.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	26.0	
Evaluator Initials : JOC			
Date: 5/15/23			

K689 - Security Assessment Services			
Vendor: Emagined			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/15/23: Bidder's blended hourly rate <b>(\$170)</b> is competitive. Their proposed sample agency cost (\$29,920) is much lower than expected, but bidder caveats this by stating that the testing is assumed to be "Level 1 Small Applications and Level 1 Testing" since the request does not provide details of the penetration tests requested.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	35.0	<p>Bidder states that the firm is a "22-year old Cybersecurity Consulting Company specializing in Penetration Testing, Managed Services and Security Assessment Services with full time resources specializing in comprehensive penetration testing of all services," "Emagined Security has logged over 175,000 hours of penetration testing and performed 10,000 penetration tests over 22 years with the average pen tester experience at 10+ years," and "Emagined Security has extensive experience in Web Application Penetration Testing, Network Penetration Testing, SCADA, API, Mobile, Wireless and Web Socket Penetration testing as well as extensive OSINT experience" (Exhibit A-2, pg. 1). Bidder also provides seven references (Exhibit A-2, pgs. 5-6), which includes two Washington state agencies, two Washington local governments, and a local government from California. All of these references included penetration testing of various types of assets (e.g., web applications, internal network, external network), and are not described as having penetration testing as just a small portion of a larger, compliance-oriented engagement.</p> <p>Bidder lists summary methodology along with their proposal for the sample agency (Exhibit C), and in doing so, describes the work that this engagement would entail in good detail. Notably, bidder acknowledges that SCADA testing would be in a production environment, and states "additional care will be provided to ensure systems are not exploited or aggressive testing does not create system stability issues." Bidder also lists the staffing/resources that would be provided for the sample engagement (pgs. 8-9), which would include 1 coordinator, one lead penetrtion tester, 2 senior web application penetration testers, 1 [additional] web application penetration tester, and 1 network penetration tester. All of the penetration testers will have at least Certified Ethical Hacker certifications, while the lead tester and the two senior web application testers will have OSCP certifications. The thick client testing would be conducted by the two senior testers.</p> <p>Bidder later states "Emagined Security Project managers have over 25 years of experience working with Penetration testing" (Exhibit C, pg. 8).</p> <p>Bidder also states in Exhibit C that they employ "over a dozen penetration testers and can staff multiple engagements of this size simultaneously."</p> <p>In Exhibit D (pg. 4), Bidder states "Our more experienced team members have been performing penetration testing and ethnical hacking engagements for over 30 years. ... For the State of Washington, over the past 7 years, Emagined Security has performed over 70 Penetration Test engagements <b>including hundreds of web applications, thick-client, API tests, mobile applications, Wireless, Mainframes</b> [emphasis added by reviewer] and thousands of internal and external network IPs tested for Cities, Counties, State Agencies, and Hospitals located in the State of Washington. ... In Addition to the State of Washington, Emagined Security has performed Penetration testing for other States Auditor Offices as well as Cities and Counties in California, Texas and Arizona. ... Our expertise is recognized internationally through the CREST organization. Additionally, Paul Underwood one of our lead Project Managers, sits on the Board of the CREST organization. A worldwide organization that certifies both Penetration testers and organizations for comprehensive penetration testing methodologies and abilities. ... Emagined Security performs hundreds of Web Application Penetration Tests, Network Penetration Tests, API &amp; Mobile Penetration tests, Mobile, Secure Code, Mainframe, Vulnerability Assessments and Wireless Assessments every year. This type of testing continues to be a core service Emagined Security offers." Bidder also states that the consultants they assign to penetration tests in Washington <b>only</b> conduct penetration testing, and then <b>lists numerous certifications their testers have which are specific to penetration testing (e.g., C EH, OSCP, OSWE, OSEP, etc.)</b>. Bidder also discusses experience testing ICS/SCADA/OT (Exhibit D, pgs.6-7).</p> <p>Bidder provides five representative projects (Exhibit D, pgs. 9-15), all of which include penetration testing. Of these, at least 2 different projects were of government organizations, 2 were private organizations that operate in areas that also have government organizations, and one was a project on a very large global software vendor. The engagement for the global software vendor required a CREST certified penetration testing company. Collectively, these projects included testing of web applications, thick clients, SCADA systems, external and internal networks, IoT devices, and firewall reviews. The sizes of these projects ranged from very small (2 weeks) to very large (12 weeks). For one of these projects, bidder states "Rules of Engagement are still used on these small CI engagements. <del>Emagined Security believes even small engagements should be treated as valued test opportunities and Emagined Security uses the same care and diligence on these small tests to provide value.</del> " <b>This suggests a consistent level of diligence among</b></p>
Staffing (30%)	30.0	30.0	Bidder provides resumes for 12 individuals (Exhibit D, pgs. 6-24), all of whom are listed as having direct experience conducting penetration tests. All testers are noted as having network penetration testing and experience, and most with web application testing experience. But notably, this list of resumes includes Patrick Cleary, who is listed as having extensive experience testing thick clients, ICS/SCADA systems, and mainframes; Ramces Chirino and Arthur Borrego, who are listed as having extensive experience testing thick clients; Felix Alcalá, who is listed as having extensive mobile testing experience; Cory Dixon, who is listed as having extensive thick client and mobile testing experience; and Ishmael Malik, who is listed as having experience testing thick clients, mainframes, and ICS/SCADA.
Qualifications Section Total Score	65.0	65.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	Bidder's sample report includes an executive summary, as well as areas of strength and areas of improvement, broken down by each area of testing (internal network, external network, application). Detailed findings include a severity level as well as a level of difficulty to exploit. Findings also include detailed descriptions (which often include context specific to the tested asset), supporting evidence (screenshots), recommendations, and additional references. However, the report did not specifically identify tests performed that <b>did not</b> result in findings.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	77.0	
Evaluator Initials : JOC			
Date: 5/15/23			

ERM			
K689 - Security Assessment Services			
Vendor: ERM			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/15/23: Bidder's blended hourly rate (\$175.00) is competitive, and their quote for the sample agency (\$42,000) is lower than would be expected.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Bidder states (pg. 12) they have 25 years of experience providing cybersecurity services, including penetration testing, and has served hundreds of clients in industries that include government, higher education, transportation, and healthcare. Bidder lists common staff certifications on pg. 13, but only one of these (C EH) is specific to penetration testing, while the rest are more generic (e.g., CISA, CISSP, CIA, etc.). (One of the resumes later in the document also lists the OSCP certification). Bidder lists three references on pg. 16 - two of whom are government organizations - but these engagements are only described here as "Penetration Testing and PCI DSS services."  Bidder's methodology (pgs. 22-34) is well detailed, covering each of the types of assets listed in the sample agency (web applications, mobile, thick clients, networks, ICS). However, <b>bidder does not list experience conducting testing on mainframes with the exception of section 5 on pg. 30, wherein mainframe testing is included under internal network penetration testing.</b>  Bidder states they have performed penetration testing services for more than 20 years (pg. 37).  Bidder lists five sample projects on ogs. 38-39. <b>Of these, 3 (Miami-Dade, Metropolitan Washington Airport Authority, Assurant) do not mention penetration testing of applications, suggesting that these may have only included network testing. The other two (City of St. Petersburg, CJCC) had application testing that appeared to be limited to web applications (i.e., no mention of thick clients or mobile applications, or of mainframes).</b>
Staffing (30%)	30.0	24.0	Bidder provides resumes for five individuals (pgs. 40-44). Of these, all five (Esteban Farao, Chris Sanchez, Divyansh Arora, Collin Connors, and Aviral Sharma) have direct experience conducting penetration tests. <b>This includes direct mention of web applications, network testing, mobile applications, and IoT devices, but there were no explicit references to tests conducted on thick clients or mainframes.</b>
Qualifications Section Total Score	65.0	45.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	Bidder provided a sample internal network penetration test report, however this did not include sample results for application testing (in fact, the report explicitly states that application-specific attacks were not conducted as part of the engagement). The report included an executive summary with some summary-level findings, but did not discuss areas of strength. The detailed findings include a "Security Level" rating (along with a CVSS2 score), but this does not more thoroughly break down the result by severity and likelihood/difficulty. The finding explanations and recommendations are well detailed, and the report provides supporting references. However, the results do not provide cited evidence (e.g., screenshots) to allow a recipient to see how they can recreate/validate the finding. The report also features very little information about the test's methodology or the steps taken to identify the findings.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	51.0	
Evaluator Initials : JOC			
Date: 5/15/23			



K689 - Security Assessment Services			
Vendor: GSG			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.
			JOC 5/15/23: Bidder's blended hourly rate (\$340.63) is <b>extremely high</b> , and the sampled agency cost (\$298,352.00) is more expensive (or almost more expensive) than the very largest engagements we have conducted, which consisted of dozens of applications. At this cost, it would probably be untenable to conduct the number of audits we aim to conduct, whether as defined by the contract, or as defined by our own performance expectations. Bidder also lists, as an assumption, that they would propose a "2% annual escalation for the proposed hourly bill rates from the second year to provide the most competitive pricing for the entire contract duration." That suggests that the blended rate would increase to \$347.44 in a year, which would further compromise our ability to conduct these audits.  Vendor then lists as an assumption: "The GSG cyber team believes that the majority scope of work can be successfully accomplished remotely utilizing virtual meeting/conference(s). GSG estimates two trips for any onsite related tasks. If, for any reason, any additional onsite trip is required then we would determine the specific need for onsite work and the corresponding accurate travel cost. We will charge for actual travel costs as per the IRS / Federal Travel Regulation. For understanding purpose, 1 trip of 3 to 5 days per person travel costs around \$1750 including flight, lodging, meals, etc." <b>However, this assumption may itself violate the requirement to submit a single, blended hourly rate as part of the RFQQ.</b>
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Bidder proposes to sub-contract with Google Mandiant to provide the requested services, stating that this arrangement enables their team to conduct network, thick client, mainframe, operational technology, and web application security testing (pg. 3).  Bidder's methodology (pgs. 30-39) for the sample agency includes sections discussing external network testing, internal network testing, web application testing, thick client testing, SCADA/ICS testing, Firewall Configuration Reviewing, and Wireless Testing. However, it also includes methods that were not required as part of the sample state agency, such as Network Architecture Review, Social Engineering, and a Physical Security Assessment. This methodology section is also poorly built and difficult to follow, as it lists considerable detail in large, sprawling paragraphs rather than smaller, more discreet, paragraphs that are better organized. Additionally, the methodology frames the sample engagement as being a test of SAO's network, which ignores the scope of work as described in the RFQQ (i.e., a sample state agency that SAO will audit).  In response to the RFQQ's work plan requirement, bidder states, in part (pg. 39): "We will provide you with services such as internal/external device/network vulnerability assessment and pen testing, as well as application-level pen testing provided by SAO's." As written, this suggests that SAO may be providing application-level pen testing, which is a fundamental misunderstanding of the intent of this RFQQ and the ensuing proposal.
			Bidder lists 11 customers under the "Qualifications" section (pgs. 43-44), but only lists 5 of them as explicitly receiving penetration testing (Lansing Board of Water and Light, Jacksonville Aviation Authority, Fort Wayne-Allen County Airport Authority, US Department of Agriculture, Department of Health and Environment). Bidder lists five representative projects (pgs. 45-50), and while all five included penetration testing, they were only a portion of the overall engagements. Of these, none listed testing on mainframes or thick client applications, and only one (Lansing Board of Water and Light) listed testing on mobile applications or SCADA. Bidder lists resumes for three individuals (pgs. 55-66). Of these three, one (Vatsal Shah) has extensive penetration testing experience, one (Kumar Setty) has limited penetration testing experience, and the third (Vicki Shah) operates in a project management capacity. <b>However, the resumes do not specify any experience testing thick clients or mainframes, and only one resume (Vatsal Shah) lists experience testing mobile devices or SCADA/ICS.</b>  Resumes for specific staff that would be provided by Mandiant are not included in the proposal.
Staffing (30%)	30.0	18.0	
Qualifications Section Total Score	65.0	32.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder provided an external network and application test (pgs. 68-95). The report's executive summary lists key observations that identify areas of strength (pg. 71), as well as recommendations to address areas for opportunity. The detailed results include a severity rating (which appears to be based off CVSS), as well as a skill level needed/ease of exploit for each finding. The descriptions are brief and do not contain considerable context, but does list additional source of information, thorough solutions, and each finding has supporting evidence (screenshots) listed under the "Technical Details" section.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	41.0	
Evaluator Initials : JOC			
Date: 5/15/23			

Guidepost			
K689 - Security Assessment Services			
Vendor: Guidepost			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/16/23: Bidder's proposed hourly rate (\$350) is <b>extremely high</b> . Sample agency cost of \$56,000 is low at that hourly rate, but bidder caveats it by stating that this varies based on the size of the applications and how they are architected.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	7.0	Bidder proposes using two subcontractors for this contract: Aanko Technologies and Truvantis. Bidder states in the Organization Summary (pg. 16) that they "specialist in IT network, cyber security and assessments, penetration testing...." but is also proposing to use sub-contractors. Bidder lists certifications of its staff (pg. 31), but none of these directly relate to penetration testing, and the vast majority of them are entirely unrelated to cybersecurity. In describing itself, the bidder did not provide any indication of the years of experience its firm has conducting penetration tests or related cybersecurity assessments.  Bidder lists five representative projects (pgs. 42-43), but only one of them (California Department of Technology) has any mention of penetration testing. Some of the other projects reference vulnerability assessments, but these can be done by just performing a vulnerability scan and parsing through the results. Furthermore, the project that references penetration testing did not provide insight into what types of assets were tested.  <u>Aside from acknowledging the RFQQ's requirements, the bidder's proposal makes no mention of thick client applications or mainframes, makes no mention of ICS, and only mentions SCADA as part of one resume.</u>
Staffing (30%)	30.0	6.0	Bidder provides resumes for 8 individuals (pgs. 33-41), five of whom are sub-contractors. Of these eight, only two (Alex Balsoy, William Harvy Suthers III) have hands-on penetration testing experience listed, while a third (Ken Mendelson) is listed as having experience overseeing penetration tests. The remaining five resumes do not describe any experience conducting or leading penetration tests. <b>Furthermore, the experience that is listed regarding penetration testing does not provide insight into what types of systems have been reviewed by those individuals (e.g., internal networks, external networks, web applications, thick clients, mainframes, ICS/SCADA, IoT, wireless, etc.).</b>
Qualifications Section Total Score	65.0	13.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	0.0	Bidder does not provide an actual sample report. Instead, they provide a redacted table of contents (pg. 44), citing the RFQQ's page limit even though we disclosed that the sample report would <b>not</b> be included in the page limits identified in the RFQQ. The table of contents itself is not sufficient to grade the bidder in this area with any measure of reliability.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	13.0	
Evaluator Initials : JOC			
Date: 5/16/23			

K689 - Security Assessment Services			
Vendor: Inspira			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/16/23: Bidder's blended hourly rate <b>(\$169)</b> is competitive, but their cost for the sample state agency <b>(\$175,000)</b> is very high. Additionally, this blended hourly rate carries the following assumption, as listed by the bidder (Inspira Response, pg. 15): "• Our Blended Hourly Rate assumes a total of up to six (6) Industry Controls assessments, up to two (2) per year for the duration of the three (3) year contract. Inspira assumes that the effort required for these Industry Controls assessments may be equal to or lower than the effort required for the Industry Controls scope for the Sample Agency. • Our Blended Hourly Rate for agencies that do not require Industry Controls assessment is expected to be lower than the rate provided in Exhibit C. These assessments will be performed remotely. • Our Blended Hourly rate is calculated with the assumptions that the assessment will be performed for up to twelve (12) agencies per year, that do not require Industry Controls assessment, and up to six (6) Industry Controls assessments (2 per year). Inspira assumes that the effort required for these assessments may be equal to or lower than the effort required for the Sample Agency.  Bidder does not define in their proposal what they mean by an "Industry Controls assessment," but it is assumed to be entirely separate from penetration testing. As such, this blended hourly rate may not be their final, single price. <b>Additionally, their third assumption suggests that bidder may not be able to provide penetration testing services for more than 12 organization per year.</b>
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	28.0	Bidder proposes to use two subcontractors for this contract: INTEGRITI Corporation, and Strobes Security, Inc.  Bidder's methodology for the sample agency is detailed at a good level, and covers the various types of assets in-scope (e.g., web applications, thick client, mobile application, etc.). The proposal does not list experience testing mainframes, but does list experience testing thick clients, mobile apps, and SCADA systems in their representative projects. Bidder lists six such projects on pgs. 20-23, and of these, 5 explicitly listed penetration testing as a service (all except for the Semiconductor Company). Although only two of these projects provide a sense of how large the engagements were, those two (California financial services company, software development company) both featured scopes that are on par with, or even bigger than the largest organizations SAO has audited.
Staffing (30%)	30.0	18.0	Bidder provides resumes for six individuals (pgs. 24-26). Of these, X (Victor Westbrook, Bhargav Tandel, Pavan Kumar Mallem, Shiva Krishna Samireddy, and Prakash Ashok) are listed as having direct experience conducting penetration testing. <b>This includes experience testing mobile and web applications, as well as red team engagements. However, I did not see mention of testing on thick clients, mainframes, or SCADA systems within these resumes.</b>
Qualifications Section Total Score	65.0	46.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder provided a sample OT/ICS pentest report, a network penetration testing report, an internal vulnerability assessment report, a mobile application testing report, a red team report, and a web application report. The OT/ICS report did not include an executive summary, discussion of areas of strength or areas for opportunity, and does not provide a likelihood/difficulty rating for the results. The detailed results include a moderate level of explanation, and include placeholders for supporting evidence (screenshots), but the recommendations and brief and are not augmented by additional references. Bidder's network penetration testing report was similar, and while it <b>did</b> include an executive summary, it was very brief. The internal vulnerability assessment contained only a bit more detail in the executive summary, but does include additional references along with the findings. The mobile application, red team, and web application reports are similar to the internal vulnerability assessment in terms of level of detail, but they also include a rating for difficulty to exploit.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	55.0	
Evaluator Initials : JOC			
Date: 5/16/23			



K689 - Security Assessment Services			
Vendor: KPMG			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/17/23: Bidder's blended hourly rate <b>(\$155.00)</b> is competitive, and the proposed cost for the sample agency <b>(\$55,800.00)</b> is a little lower than we would expect for such an engagement.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	28.0	Bidder states "KPMG understands that SAO is embarking on this Security Assessment Services initiative to assess the relative cybersecurity maturity of the select state agencies and local governments in alignment with the state's IT security policies and standards established by the Office of the Chief Information Officer (OCIO)" (pg. 8). This is <b>NOT</b> what this RFQQ is asking for.  Proposer's sample project schedule (based off the sample state agency) is reasonable in duration, and is consistent with similar engagements we have conducted before. It also, adeptly, identifies the long lead time needed before testing to scope the work. Bidder's methodology for the proposed work (pgs. 15-27) is detailed at a good level.  Bidder proposes using a subcontractor (FYRM Associates, Inc.), but describes their services as being for ICS/SCADA penetration testing (pg. 48).  Bidder says they have been conducting penetration testing services for over 10 years, with individual testers having an average of 4-7 years of experience, and senior leaders having over 10 years of offensive security experience. Collectively, this translates to "hundreds of tests across all domains of penetration testing" (pg. 61). Bidder also lists their testers as possessing multiple different types of pentesting certifications (e.g., OSCP, CEH, etc.) in addition to more generic security and IT certifications (e.g., CISSP, CISM, CISA, etc.).  Bidder provides five representative projects (pgs. 63-65), all of which included penetration testing. While these projects included a mix of network, web application, mobile, and SCADA testing, <b>the information provided did not indicate that these projects included testing on mainframes or thick clients.</b>
Staffing (30%)	30.0	24.0	Bidder provides resumes for eight individuals (pgs. 67-75), and of these, 6 (Rahul Kohli, Daniel S. Stern, Evan Rowell, Griffin A. Reid, Christopher Day, Weston H. Cole) are listed as having experience conducting penetration testing. Among these resumes, only 2 (Evan Rowell, Weston H. Cole) discuss experience conducting penetration testing on mobile applications, only (Weston H. Cole) discuss experience testing thick clients, and <b>none of the resumes explicitly list experience testing mainframes or ICS/SCADA systems.</b>
Qualifications Section Total Score	65.0	52.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder's sample report (beginning on pg. 77) includes an executive summary that lists strengths and opportunities for improvement. The detailed findings list each finding's severity, but do not articulate the difficulty or likelihood of a vulnerability being exploited. The vulnerability details are moderately explained, with separate narratives on the technical analysis and the impact of that vulnerability, and each finding does list steps to reproduce and recommendations. However, the detailed results do not provide additional references.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	61.0	
Evaluator Initials : JOC			
Date: 5/17/23			

K689 - Security Assessment Services			
Vendor: Lumen			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/17/23: Bidder's blended hour rate (\$ <b>160.00</b> ) is competitive, and their estimated cost for the sample state agency (\$ <b>84,550</b> ) is roughly what would be expect for an engagement of that size.  <b>Note:</b> Bidder notes as early as pg. 4 that "The State of Washington has been a Lumen customer for over four decades," and says on pg. 5 "As a corporate resident of Washington state and a services provider to the state and local governments...." However, Bidder does <b>not</b> disclose non-audit services performed during the past four years as part of the response to Exhibit A-1 (pg. 22). This makes it difficult to assess potential conflicts of interest or independence issues. On 5/18, Lumen responded to a question about these non-audit services, stating they could include Centrex services, Cisco CPE, Ethernet, broadband, etc., or specifically in this case work that they put in place for state/local gov't that they could be testing. <b>This means any potential penetration test using this bidder, especially pertaining to network testing, may end up reviewing how the bidder set up those networks. Similarly, configuration reviews of network devices and firewalls using this vendor may result in the vendor evaluating their own work.</b>
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Bidder lists some of the certifications their staff possess that directly support penetration testing (pg. 44), which include GPEN, GWAPT, OSCP, and CEH.  <b>Bidder states they have experience conducting penetration testing on web applications, thick clients, mainframes, operational technology/ICS/SCADA, networks, and source code (pg. 46), as well as wireless networks (pg. 45).</b> However, Bidder does not clearly state how many such engagements they have conducted (such as a ballpark or approximate number), nor does the bidder clearly state how many years the firm has specifically been conducting penetration testing.  Bidder states their staff have an average of 7+ years of penetration testing experience.  Bidder lists five representative projects (pgs. 50-52), and of these, 4 (Sage Dental Management, Center for Dialysis Care, Penske Media Corporation, CU Direct) included penetration testing, while the fifth (Ethos Group) included a check for default credentials. These assessments included a mix of external and internal penetration testing, wireless testing, and web application testing. <b>However, the proposal does not list these engagements as having included penetration testing on thick clients, mainframes, or ICS/SCADA systems, and only two engagements (Sage Dental Management, Center for Dialysis Care) featured web application testing.</b>
Staffing (30%)	30.0	18.0	Bidder lists resumes for 5 individuals (pgs. 114-121). Of these, 4 (Mike Ramer, Tom Fulton, Keon J. Morrison, Nick Hutchison) have direct experience conducting penetration testing, while the fifth (Erik Rives) is a security consultant with experience in other areas. However, these resumes generally only list experience conducting penetration testing on networks, wireless networks, and web applications, only one resume (Keon J. Morrison) lists experience testing mobile applications and thick clients, and none of the resumes list experience testing mainframes, or ICS/SCADA systems.
Qualifications Section Total Score	65.0	39.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder provides a sample penetration test report (pg. 75). The report includes an executive summary, with areas of opportunity and areas of strength. The detailed findings include detailed explanations of the results and supporting evidence (screenshots) showing how those results were identified, as well as remediation steps. However, the findings do not include supporting references, and only provide one risk rating to each finding rather than rating them by severity and likelihood/difficulty of exploitation independently.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	48.0	
Evaluator Initials : JOC			
Date: 5/17/23			

Online			
K689 - Security Assessment Services			
Vendor: Online			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/17/23: Bidder's blended hourly rate (\$170) is competitive, and the sample agency cost (\$46,920) is lower than what would typically be expected of a scope of this size.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Bidder says their firm has "provided security testing, assessment, and advisory services" for over 36 years (pg. 5).  <b>Bidder lists a methodology for the sample engagement (pgs. 9-11), but does not state how they would approach testing on the thick client application. Bidder also states "We have successfully conducted several ICS and SCADA tests with no downtime," which does not indicate extensive experience testing those types of systems.</b>  Bidder states they have " performed hundreds of cybersecurity and penetration testing engagements for clients, including network-layer penetration testing, application-layer penetration testing, wireless penetration testing, code review, API reverse engineering, social engineering, and secure coding training workshops" (pg. 18). When describing their vulnerability assessment experience, Bidder states they have conducted vulnerability assessments on thick client applications and mainframes (pg. 19), but does not mention thick clients or mainframes when discussing their penetration testing experience (pg. 19).  Bidder lists certifications for staff which directly support penetration testing (pg. 20), including GWAPT, GPEN, CEH, and OSCP, as well as other certifications regarding security qualifications more generally (e.g., CISSP, CISA, CISM, Security+).  Bidder lists five representative projects (pgs. 21-23), all of which included penetration testing. <b>However, only one of these is listed as including SCADA systems (Louisiana Local City Government Agency), none are listed as including mainframes or thick clients, and the penetration testing on two engagements (National Health Information Network, Community College Commission) was limited to network penetration testing.</b>
Staffing (30%)	30.0	18.0	Bidder provides short resumes for eight individuals (pgs. 24-28), as well as complete resumes (beginning on pg. 88), but only 5 individuals (Will Bechtel, Warren Campbell, Michael Stringer, David Bulloch, Jason Nguyen) are listed as having direct experience conducting penetration tests, with the remaining three individuals serving in management and oversight roles. <b>Of the individuals with penetration testing experience, the resumes list experience testing networks, wireless networks, and web applications, but do not list experience testing thick clients, mainframes, or ICS/SCADA.</b>
Qualifications Section Total Score	65.0	39.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder provides a sample report (pg. 66), which includes an executive summary that lists areas of strength and areas of opportunity. The detailed findings include a moderately detailed description, a recommendation, supporting evidence (screenshots) as well as steps to reproduce. However, the results do not provide additional references, nor do they articulate the difficulty or likelihood of the vulnerability being exploited.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	48.0	
Evaluator Initials : JOC			
Date: 5/17/23			



K689 - Security Assessment Services			
Vendor: Peraton			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/18/23: Bidder's blended hourly rate <b>(\$175)</b> is competitive. Their proposed sample agency cost <b>(\$58,209)</b> is a little lower than expected.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Bidder's proposed methodology for conducting work at the sample state agency is well detailed, but doesn't provide any details specific to testing thick client applications (the proposal includes more thorough methodologies for the other types of assets, such as web applications, wireless and wired networks, and SCADA systems).  Bidder provides five sample projects (Exhibit D, pgs. 4-11), and of these, 4 (Ohio Bureau of Workers' Compensation, Sacramento Municipal Utility District, Exelon, Iconectiv) explicitly included penetration testing. These tests mainly consisted of network and web application testing, but two (Ohio Bureau of Workers' Compensation, Exelon) also included wireless assessments, and one (Exelon) included SCADA testing and (what appears to be) limited testing of a mobile application. <b>However, none of the referenced projects list testing performed on thick client applications or mainframes.</b> None of the other provided documentation addresses experience testing thick clients or mainframe applications.  Bidder's proposal does not give indication into the years of experience the firm has conducting penetration tests, nor does it provide context regarding the number of penetration tests the firm has conducted.  Certifications among key staff are listed with the resumes, and include certifications supporting penetration testing (CEH, GPEN, OSCP, etc.), as well as more generic security certifications (CISSP, etc.). However, the proposal does not include information on certification requirements or how the bidder's key staff maintain their skills or qualifications.
Staffing (30%)	30.0	18.0	Bidder provides resumes for seven individuals, six of whom (Richard Daugherty, Janine Frederick, Michael Hylkema, Stephen McNaught, Marcus Pang, Jason A. Youzwak) have direct experience conducting penetration tests. Three (Richard Daugherty, Michael Hylkema, Jason Youzwak) are listed as having experience conducting penetration testing on ICS/SCADA, and two (Stephen McNaught, Marcus Pang ) are listed as having experience testing mobile applications. However, none of the individuals are listed as having experience conducting penetration testing on thick clients or mainframes.
Qualifications Section Total Score	65.0	32.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	Bidder provided an extensive sample report covering network and web application testing, but also included a configuration review and controls assessment of the sampled systems. The report included an executive summary and some areas of opportunity, but did not include areas of strength. Much of the report's content focuses on results of the configuration review/controls assessment, with the penetration testing results buried later in the document. The structure of this report make it difficult to distinguish the various lines of work, as the content jumps from one method to another without much introduction to each, respective line of work before discussing the results. Detailed penetration test results begin on pg. 73 of the file. Each finding's observation and discussion are moderately discussed, and are supported with evidence (screenshots). <b>However, the findings do not include additional references, and do not break down their criticality by the individual finding's severity and likelihood/difficulty of exploitation. Additionally, the recommendations to remediate the issues are often very brief, often lacking step-by-step walkthroughs to help the recipient understand how to remediate the identified finding.</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	38.0	
Evaluator Initials : JOC			
Date: 5/18/23			

K689 - Security Assessment Services			
Vendor: Plante Moran			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/18/23: Bidder's blended hourly rate (\$250) is high, but the cost for their sample state agency (\$83,500) is within the range expected for an engagement of this size.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Bidder's proposal features repeated content on back-to-back pages (the attack chain and methodology content on pgs. 22-24). Bidder states that their "main area of focus is on manual techniques..." (pg. 25), which is precisely the kind of expertise this RFQQ is looking for.  Bidder's proposed methodology (pgs. 25-29) is written at a high level, making it easy to understand but slightly less demonstrative of the bidder's technical qualifications.  Bidder also has multiple references to SAO as if SAO were the targeted entity: "SAO's IT department" and later "We will perform a review of ASO's (sic) network design..." (pg. 28), "This is a pont-in-time security assessment of SAO" (pg. 29), etc.. These suggest a misunderstanding of the type of work this RFQQ is looking for (i.e., penetration testing of state agencies and local governments as part of SAO audits).  Bidder states (pg. 36) that their "cyber professionals have, on average, more than 13 years of experience performing cybersecurity control evaluations, IT compliance testing, internal audit assistance, technical assessments, and internal control consulting services," however this does not clearly identify how much experience their firm or staff have conducting <b>penetration testing</b> specifically. Bidder also lists some of the certifications their staff have (pgs. 36-37), which include certifications supporting penetration testing (CEH, GPEN, etc.), as well as more generic IT/Security certifications (CISSP, Security+, etc.).  Bidder lists five representative projects (pgs. 40-44), all of which included penetration testing, most of which was network testing and web application testing. However, one of the engagements (City of Tacoma) only included network penetration testing, only one engagement (Ohio Public Employees Retirement System) included wireless testing, <b>and none of the engagements listed testing on thick clients, mainframes, mobile applications, or ICS/SCADA. Bidder does not reference thick clients or mainframes at all in their proposal (aside from including the lanuage from SAO's RFQQ), and does not provide examples of actual/completed tests on ICS/SCADA svstems or mobile applications.</b>
Staffing (30%)	30.0	12.0	Bidder provides resumes for 9 individuals (pgs. 47-50), but of these, only 5 (Saumil Shah, DeShaun Ormond, Shayna Harbecke, Mícheál Sheridan, Parth Doshi) are listed as having direct experience conducting penetration testing. <b>Of these five, only 1 (Saumil Shah) has experience conducting mobile application testing; the remaining four individuals are either listed as having experience with network and web application testing, or do not have specific areas of penetration testing listed. None of the resumes noted experience conducting penetration testing on thick client applications, mainframes, or ICS/SCADA.</b>
Qualifications Section Total Score	65.0	26.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	3.0	Bidder provides a sample report (pg. 87) of a network penetration test. The report includes an introduction, but did not articulate areas of strength or summary level areas for improvement. The detailed results only included four findings, but one of them is just the results of a vulnerability scan, making the sampled report very cursory compared to the type of work that is typically included in penetration tests as part of SAO audits. The detailed results include a description, a recommendation, and screenshots (supporting evidence), but the descriptions are very brief and do not provide much context. Furthermore, the findings do not provide references to additional sources of information (e.g., vendor or best practice websites), and the results are only given a risk rating rather than individual severity and likelihood/difficulty ratings.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	29.0	
Evaluator Initials : JOC			
Date: 5/18/23			

K689 - Security Assessment Services			
Vendor: RSI			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/18/23: Bidder's blended hourly rate <b>(\$215)</b> is reasonable, but their proposed cost for the sample state agency <b>(\$99,330)</b> is higher than would be expected for a scope of this size.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Bidder notes (Exhibit A-2) that some of their clients include local governments in Washington (and possibly Washington state government agencies - the language can be read multiple ways), but does <b>not</b> disclose these as non-audit services in Exhibit A-1.  Bidder proposes using a subcontractor, NetSPI, LLC, for penetration testing services.  Bidder proposes a sample methodology that lists the main penetration testing steps with varying levels of detail (Exhibit C, pgs. 3-11); the sections discussing network testing are much more thorough than the sections describing web and mobile application testing. <b>However, the section that discusses testing on OT devices from inside the network is concerning in that it does not acknowledge the sensitivity or fragility of certain OT/ICS/SCADA systems and the impact that penetration testing (including automated scans) can have on those systems.</b> Since these systems often serve critical infrastructure functions, testing them requires a heightened level of care and awareness.  Bidder lists five representative projects (Exhibit D, pgs. 4-11), but of these, only 3 included penetration testing, and were limited to the following scopes: 1. "Anonymous Telecom Corporation" included external & internal penetration testing, but the description does not state if this included any application testing. Furthermore, the penetration testing seems to have been a relatively small portion of a larger IT security assessment. 2. "Leading Financial Services Firm": Internal network penetration test 3. "Merger & Acquisition": Internal and external penetration testing, and testing on two web applications. <b>None of the cited projects, as well as other parts of the bidder's submission, provides specific examples or instances of penetration testing completed on thick clients, mainframe, mobile applications, or ICS/SCADA systems.</b>
Staffing (30%)	30.0	18.0	Bidder provides resumes for 8 individuals (Exhibit D, pgs. 11-12), seven of whom explicitly list direct experience conducting penetration tests. According to the resumes, the penetration testing experience for most of these seven individuals consists of network and web application testing; however, one (Eric Gruber) is listed as also having experience testing thick clients, two (Eric Gruber and Benjamin Tindell) are listed as having experience conducting mobile testing, and one (Larry Trowell) is listed as having experiente testing IoT devices. None of the individuals, however, are listed as having experience testing mainframes or ICS/SCADA systems.
Qualifications Section Total Score	65.0	32.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	Bidder provided a sample network penetration test report, and a sample web application penetration test report. The sample network testing report includes an executive summary that lists areas of opportunity, but does not list areas of strength. The detailed findings include moderate discussion of the results, with both vulnerability details and an impact statement, as well as thorough recommendations, extensive screenshots (evidence), and additional references. However, the each finding is only rated by a single severity grade, rather than by distinct severity and likelihood/difficulty levels. The sample web application report was similar in nature, but also included a table of the OWASP top 10 vulnerabilities, showing whether or not each of those vulnerabilities was identified during the test.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	44.0	
Evaluator Initials : JOC			
Date: 5/18/23			



K689 - Security Assessment Services			
Vendor: SAC			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/18/23: Bidder's blended hour rate (\$120) is very competitive, and their projected cost for the sample state agency (\$24,000) is very low.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Bidder's cover letter states "Recently we successfully completed an extensive Cybersecurity Maturity Assessment involving penetration testing and NIST assessment for Pierce County's network infrastructure supporting their MIS, Industrial Control Systems and Cloud applications." However, Bidder does not list any non-audit services conducted for state agencies or local governments in Washington in Exhibit A-1.  Bidder lists some of their certifications (Exhibit D, pg. 5), which include CEH, GWAPT, GPEN, and OSCP.  Bidder lists their approach to penetration testing and their methodology (Exhibit D, pg. 6), but it is very high level, and does not contain many details about what methods the bidder would use to carry out those steps. (Note: This approach appears to be repeated on pgs. 15-16).  Bidder lists seven represnetative projects (Exhibit D, pgs. 12-14), however, only three are listed as having penetration testing. Of these three, one (Large WA County) is listed as having had penetration testing on internal and external networks, as well as cloud applications and ICS/SCADA systems, while the other two (Large County Service Authority, Technology Company) do not specify what types of assets received penetration testing. <b>Aside from a sample report, this is the only reference to work completed on any ICS/SCADA systems in the bidder's submission, and the bidder's submission does not reference experience conducting testing on thick client applications, mainframes, or mobile applications at all.</b>
Staffing (30%)	30.0	12.0	Bidder provides resumes for five individuals (Exhibit D, pgs; 19-24), but of these, only two are listed as having direct experience conducting penetration tests. One (Robert Henderson) is listed as a web application penetration tester, while the other (William Price) is listed as an internal/external testing specialist. <b>However, neither resume mentions any experience testing thick client or mobile applications, mainframes, or ICS/SCADA systems.</b>
Qualifications Section Total Score	65.0	26.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder provided a sample ICS penetration test report and a sample internal network penetration test report. (Bidder also provided a sample NIST Cybersecurity Framework Control Assessment Report, but this was not reviewed because it falls outside the scope of the services requested by this RFQQ). The sample ICS report is <b>very</b> brief (10 pages total, including cover page and table of contents), and only discusses two results: Industrial System Access and Battery Backup Access. The methods to assess and identify these results are technical in nature (e.g., default credentials, accessing devices through a VPN), and both results include recommendations. <b>But the results are categorized by their "Threat Description" level, rather than by individual severity and likelihood/difficulty ratings. The results also do not include references to external sources. The report itself, though short, also does not discuss areas of strength.</b> The sample network penetration test report included an Executive Summary/Testing Summary, which included areas of strength and areas for improvement. The rest of the report was consistent with the sample ICS report in terms of the level of detail presented in the results.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	35.0	
Evaluator Initials : JOC			
Date: 5/18/23			

Shorebreak			
K689 - Security Assessment Services			
Vendor: Shorebreak			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/18/23: Bidder's blended hourly rate <b>(\$163)</b> is competitive, but their proposed price for the sample state agency <b>(\$136,240)</b> is very high for a scope of that size.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Bidder states that they would use a proprietary web application titled Lifeguard (pg. 7) to report results to auditees in real time. <b>Use of this method would likely require extensive conversations to gauge its security and data retention/deletion protocols.</b>  Bidder state that they have been the "exclusive penetration test provider for NOAA's National Weather Service since late 2014, testing all national mission critical systems thoroughly while ensuring no impact to operations from testing. We conduct external, internal, web application, social engineering, and various other types of testing for NOAA's National Weather Service, and are the only entity to conduct this level of testing on the national mission critical forecast centers such as the National Tsunami Warning Center, Storm Prediction Center, National Hurricane Center, Pacific Tsunami Warning Center, Space Weather Prediction Center, and others. These centers are 24/7 forecast centers that have operational networks that require constant availability so that severe weather is accurately predicted and weather products are disseminated in a timely manner." (pg. 23).  Bidder's methodology for network penetration testing is well detailed (pgs. 29-31), but their methodology for assessing web applications is not detailed at all (pg. 31).  Bidder states their penetration testers collectively have over 30 years of experience conducting penetration testing. Bidder lists the certifications their team possesses, which include certifications that directly support penetration testing (e.g., CEH, CWAPT) as well as more generic IT/Security certifications (e.g., CISSP, Security+).  Bidder provides five representative examples (pgs. 42-48), all of which included penetration testing. However, based on the descriptions, these engagements appeared to be limited to network penetration testing (external and internal), with some web application testing as well. <b>The projects did not reference testing on thick client or mobile applications, mainframes, or ICS/SCADA.</b>
Staffing (30%)	30.0	12.0	Bidder provides resumes for eight individuals (pgs. 49-52), but only four of them (Nicholas V., Erik R., Brad B., Alberto R.) list experience directly conducting penetration testing. Of these, two (Nicholas V., Alberto R.) have experience conducting red team engagements, but only one (Erik R.) is explicitly listed as having experience conducting penetration testing of web applications (Note: Alberto R. is listed as having experience with "application security threat hunting," but this does not come across as penetration testing). <b>None of the listed resumes indicate experience testing thick client or mobile applications, mainframes, or ICS/SCADA systems.</b>
Qualifications Section Total Score	65.0	33.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder provided a sample report covering external and internal network penetration testing, as well as penetration testing of a mobile application and a web application. The report includes an executive summary, and discusses areas for opportunity via summary level results (pgs. 9-18), as well as a very brief summary of areas of strength (pg. 18). The detailed results themselves (e.g., the web application findings beginning on pg. 35) include descriptions of the findings and their impact, supporting evidence (e.g., screenshots), and recommendations of varying levels of detail. However, they do not list references to sources for additional information, and they are assigned a single risk rating rather than individual severity and likelihood/difficulty ratings.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	42.0	
Evaluator Initials : JOC			
Date: 5/18/23 - 5/19/23			

Soteria			
K689 - Security Assessment Services			
Vendor: Soteria			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/19/23: Bidder's blended hourly rate (\$272) is high, and their proposed cost for the sample state agency (\$125,936) is also considerably higher than would be expected for a scope of this size.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	28.0	Bidder states (Exhibit A-1) they have performed a statewide Microsoft Security Remediation Project for WaTech.  Bidder states (Exhibit A-2) that the firm has been in business since 2014. Bidder also lists a subcontractor (Katalyst) for "Information Technolgy - Infrastructure Design/Network."  Bidder adeptly notes in their sample proposal that "Due to the critical nature of ICS, intensive/aggressive scanning and enumeration are not performed; instead, only lightweight scanning and fingerprinting techniques are used. Additionally, exploitation of identified vulnerabilities are not performed; the conditions for exploitation will be demonstrated without actual execution" (Exhibit C, pg. 5). However, the Bidder describes the remainder of their methodology at a fairly high level (Exhibit C), and does not provide any methodology specific to testing thick clients, mobile applications, or mainframes.  Bidder provides five representative projects (Exhibit D, pgs. 3-6),all of which included penetration testing. However, two of these (Projects 3 and 4) are listed as only having external/internal network testing, and one (State of South Carolina - Department of Administration) does not specify what types of assets were tested. <b>The other two engagements (South Carolina State Election Commission, Project 5) featured broader scopes, collectively including testing on web applications, thick clients, mobile applications, wireless, ICS/OT devices, and hardware testing. However, the bidder does not provide any examples of testing on mainframe systems.</b>  Bidder lists their staff certifications (Exhibit D, pg. 11), which include certifications that support penetration testing (e.g., CRT0, CRTP, OSCP), and certifications that support IT/cybersecurity more generally (e.g., CISSP, Security+, etc.).
Staffing (30%)	30.0	18.0	Bidder provides resumes for 11 individuals (Exhibit D, pgs. 12-34), 7 of whom list direct experience conducting penetration testing. Of these, two (Scott Thomas, Mike Dame) has experience on Red Team engagements, one (Paul Ihme) has experience conductive offensive operations for the U.S. government, two (Mike Dame, Jevin Eskridge) are listed as having experience testing web applications, one (Mike Dame) is listed as having experience testing mobile applications and wireless, and one (Scott Thomas) also has experience conductive penetration testing on ICS devices. <b>However, none of the individuals are listed as having experience conducting penetration testing on thick clients or mainframes.</b>
Qualifications Section Total Score	65.0	46.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	Bidder provides a sample report from a Red Team engagement, but it does not explicitly note testing on applications of any kind (e.g., thick clients, web applications, mobile), nor does it note testing on mainframes or ICS/SCADA systems. The report provides an executive summary, and later lists outcomes of tests (pg. 9) showing which methods ended up resulting in positive versus negative outcomes. The detailed results are not presented in the way that a typical penetration test report is built; while the results have descriptions, supporting evidence (redacted screenshots), and recommendations, <b>they do not have severity ratings (either severity itself or likelihood/difficulty of exploitation)</b> . The findings also do not list additional sources of information about those results.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	52.0	
Evaluator Initials : JOC			
Date: 5/19/23			



K689 - Security Assessment Services			
Vendor: Spirent			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/22/23: Bidder's blended hourly rate <b>(\$160)</b> is competitive, and their estimated cost for the sample state agency (\$70.400) is within the range of what would be expected of an engagement of that size.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	21.0	Bidder's proposal does not explicitly list how long the firm has been conducting penetration testing, or provide a summary of how many penetration test engagements the firm has conducted over the years.  Bidder's methodology for the sample state agency is quite thorough, outlining the steps the bidder would take to test each of the types of assets included in the scope.  Bidder states that they would use a proprietary web portal titled (Exhibit C, pg. 17) to report results to auditees in real time. <b>Use of this method would likely require extensive conversations to gauge its security and data retention/deletion protocols.</b>  Bidder lists the credentials their staff possess (Exhibit C, pg. 21), which include some in direct support of penetration testing (OSCP, GPEN, etc.) and others that are more generic to IT/Security (CISSP, GICSP, etc.).  Bidder's qualifications response is thorough in terms of the methods the bidder would employ for conducting vulnerability assessments and penetration testing (Exhibit D, pgs. 1-16). <b>However, this response does not explicitly address testing thick client applications or mainframes, nor does the bidder reference experience conducting testing on those system types.</b>  Bidder lists five representative projects (Exhibit D, pgs. 19-21), all of which included penetration testing. All included network testing (external and internet), 2 (Public Utility District and City Government (Project 3)) included wireless testing, 2 (City Government (Project 1), US Transit Authority) included testing on applications, with the latter including mobile application testing, and 3 (Projects 2, 4 and 5) included testing on ICS/SCADA systems. <b>However, these projects do not explicitly list testing on thick client applications or mainframes.</b>
Staffing (30%)	30.0	18.0	Bidder provides resumes for 6 individuals (Exhibit D, pgs. 26-41), all of whom have direct experience conducting penetration testing. All list experience conducting network penetration testing, most (Habib Ullah, Prashantkumar Nattanmai, Shiv Shankar Ganapathy, Tej Aulakh) list experience testing web applications, two (Joshua Brown, Tyler Bennett) list experience testing embedded devices, and two (Prashantkumar Nattanmai, Shiv Shankar Ganapathy) list experience testing mobile applications. However, none of the provided resumes explicitly list experience testing thick client applications or mainframes.
Qualifications Section Total Score	65.0	39.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	9.0	Bidder provides a sample report for a mobile application penetration test (Exhibit D, pg. 42), a sample network test report (pg. 66), and a web application penetration testing (pg. 95). Bidder also provided a sample report for a source code scan (pg. 79), but this was not reviewed because it falls outside the scope of the services requested by this RFQQ.  The mobile application report includes a summary statement of risk (which might be considered an executive summary), but it does not identify areas of strengths/areas for improvement. The detailed results include an overall severity level that appears based on CVSS, but does not explicitly list the likelihood/difficulty of that vulnerability being exploited. The results include descriptions of the findings and sometimes their impact, screenshots (additional evidence), thorough recommendations, and additional references for some findings. Some of the findings rated "Low" severity, however, do not include written narrative explaining them, indicating an inconsistent level of detail put into articulating the various results.  The network penetration test and web application test reports were similar in nature to the mobile application report, with the findings exhibiting varying levels of detail in the aforementioned areas.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	48.0	
Evaluator Initials : JOC			
Date: 5/22/23			

Summit			
K689 - Security Assessment Services			
Vendor: Summit			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/22/23: Bidder's blended hourly rate (\$240) is high, and their estimated cost for the sample state agency (\$115,200) is higher than what would be expected for an engagement of that size.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Bidder's proposed workplan (Exhibit C, pgs. 9-15) describes the test approach at a moderate level, and does not list varying approaches for testing the mobile, thick client, and web applications listed in the scope of the sample state agency.  Bidder provides examples of completed projects (Exhibit D, pgs. 1-7) to demonstrate knowledge, including five listed under penetration testing (pgs. 3-7). Each of these five projects includes a scope that appears narrower than the sample state agency, with two (Projects 1 and 2) consisting of internal network testing, two (Projects 4 and 5) consisting of web application testing, one (Project 3) consisting of a penetration test on a thick client, and one (Project 2) testing SCADA systems. These projects do not list any kind of timelines to articulate how long they took or how recent they were. <b>Additionally, the projects do not include testing on mainframes or mobile applications, and the bidder only mentions mobile application testing under the assumptions/requirements section (pgs. 9-10).</b>  Bidder's proposal does not explicitly list how long the firm has been conducting penetration testing, or provide a summary of how many penetration test engagements the firm has conducted over the years, and does not list certifications for staff beyond what is listed in the provided resumes (graded below).
Staffing (30%)	30.0	12.0	Bidder provides resumes for eight staff, but of these, only 5 list direct experience conducting penetration testing. Of these, the majority (Oscar Gutierrez, Thom G. Hastings, Heidi Metzler, Jacob Porter) are listed as having experience in either network testing, web application testing, or both, and only one individual (John W. Osborn) is listed as having experience testing other types of assets, including ICS devices and mainframes. However, none of the individuals are listed as having experience testing thick client applications or mobile applications.
Qualifications Section Total Score	65.0	26.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	Bidder provides a sample application and network penetration test report, which includes an executive summary and general recommendations (areas for improvement), but does not include a summary of areas of strength. The detailed results include an overview of each finding, a discussion of impact and its severity rating, a separate discussion and rating of that finding's likelihood to be exploited, a thorough walkthrough of how to identify/reproduce the results (including supporting evidence), a rating for the level of effort to remediate the finding, and recommendations. However, while the report does contain links to additional references, these are listed as an appendix, rather than with the relevant findings.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	38.0	
Evaluator Initials : JOC			
Date: 5/22/23			

SystemSoft			
K689 - Security Assessment Services			
Vendor: System Soft			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/22/23: Bidder's blended hourly rate <b>(\$150)</b> is competitive, but their estimated cost for the sample state agency <b>(\$285,000)</b> is extremely high; such a cost would be prohibitively expensive for SAO to pay if it were to attempt to audit the number of entities articulated in the RFQQ. <b>Furthermore, bidder does not provide any kind of workplan or project plan to articulate how they arrived at such a high price.</b>
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	12.0	Bidder says the firm has over 20 years of experience in cybersecurity (Exhibit D, pg. 3), but does not specify how many years of experience they have conducting penetration testing.  Much of the bidder's proposal is for content that is extraneous from the penetration testing services requested in the RFQQ, or which mistakenly frames the work as occurring on SAO systems rather than on systems of organizations that SAO audits (see Exhibit D, pgs. 7-10).  Bidder lists six representative projects in summary form (Exhibit D, pgs. 4-5). Bidder also lists three of these (State Department of Revenue, State Community College, State Department of Human and Health Services) as case studies at the end of their proposal (Exhibit D, pgs. 25-30). Based on both sets of information, only three organizations listed (Superior Court of California, North Carolina Department of Health and Human Services, Fayetteville Technical Community College) explicitly list penetration testing; a fourth (North Carolina Department of Revenue) lists "Administering mainframe testing" (Exhibit D, pg. 25), but whether or not this was penetration testing is unclear. The remaining engagement (Pennsylvania Turnpike Commissions) did not list penetration testing as part of the work performed, and the Department of Revenue did not list any additional penetration testing beyond what it stated for mainframe testing. Of the three organizations that definitively list penetration testing, the total body of work collectively included external network penetration testing, internal network penetration testing, wireless penetration testing, and web application penetration testing. <b>None of the referenced examples referenced testing on thick client applications, mobile applications, or ICS/SCADA systems, and penetration testing on these types of systems is also not mentioned in any other part of the proposal.</b>  Bidder only lists certifications within the resumes for four of its staff (which are graded separately below). Among these three staff, certifications include a few that support penetration testing specifically (CEH, OWASP Specialization) as well as a few that support IT/cybersecurity more generally (CISSP, Security+).
Staffing (30%)	30.0	6.0	Bidder lists resumes for 6 individuals (Exhibit D, pgs. 15-20), but of them, only one (Praneetha Kantu) list direct experience conducting penetration testing (network and application). Two others (John Nykaza, Craig Wilson) list penetration testing/red teaming as a competency, but do not list experience conducting penetration tests. Additionally, none of the resumes indicate experience conducting penetration testing with thick clients, mainframes, mobile applications, or ICS/SCADA systems.
Qualifications Section Total Score	65.0	18.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	3.0	<b>Bidder does not provide a sample report, but instead provides only four screenshots of various pages from a report.</b> The first screenshot (Exhibit D, pg. 21) is just a table of findings with an associated risk rating and expected remediation date (unsure as to who defined these dates). The second screenshot is of a detailed finding (pg. 22), showing a brief description, a moderately-described impact statement, and a brief recommendation, but no supporting evidence (e.g., screenshots), a "Final risk rating" rather than discreet ratings for severity and likelihood, and no additional references. The third screenshot (pg. 23) is similar, and while it does show a screenshot, it does not show the recommendation (and therefore the depth or detail of the recommendation). The fourth screenshot (pg. 23) is also a table with four sampled findings, each of which contains a brief description, suggested mitigation steps, and impact on confidentiality/integrity/availability. <b>The provided sample content did not include an executive summary, summary of strengths/areas of improvement, methodology, or explanation of what went into categorizing the identified findings.</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	21.0	
Evaluator Initials : JOC			
Date: 5/22/23			



K689 - Security Assessment Services			
Vendor: Tevora			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/22/23: Bidder's blended hourly rate (\$250) is high, but their estimated cost for the sample state agency (\$72,640) is within the range of what would be expected for an engagement of this size.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	14.0	Bidder states in their cover letter (pg. 2) that they are prepared to provide internal and external penetration testing, mobile application penetration testing, and web application penetration testing. <b>However, this implicitly does not include penetration testing on thick clients, mainframes, or ICS/SCADA systems.</b>  Bidder provides a workplan for the sample state agency that discusses methodology in moderate detail. However, whereas the workplan consists of individual sections for testing the internal/external networks, web applications, and mobile application in the sample agency's scope, the workplan does <b>not</b> include sections discussing methodology for testing the thick client or ICS/SCADA that are within the sample scope. Furthermore, the pricing table the bidder submits (pg. 35) includes internal penetration testing, external penetration testing, mobile application penetration testing, and web application penetration testing as line items, but does not include testing of the thick client or ICS/SCADA systems as line items.  Bidder does state in the qualifications section (pg. 39) that they have the experience to test the full range of system types the RFQQ requests services for, saying "We also have expertise in penetration testing, covering web applications, thick client applications, mainframes, network, source code, Industrial Control Systems (ICS), Medical equipment, Supervisory Control and Data Acquisition (SCADA), and other Operational Technology (OT) that reside within local government and medical facilities." <b>However, the exclusion of thick client testing and ICS/SCADA testing, both in their cover letter as well as in their workplan (including the price table) indicates that the bidder is not prepared to offer testing on thick clients, ICS/SCADA systems, or mainframes.</b>  Bidder states (pg. 39) their staff possess certifications such as CEH and OSCP; these directly support penetration testing.  Bidder provided five representative projects (pgs. 46-55), all of which included network penetration testing, and including two (County Government in California, City Government in California) that included wireless testing, and three (City Government in California, Major Corporation who specialize in Advanced Analytics for Process Manufacturing located in Washington, Best-in-Class Gaming Retailer located in Washington) which included web application testing.
Staffing (30%)	30.0	12.0	Bidder provides resumes for 3 individuals (pgs. 56-58), but only one of them (Kevin Dick) is listed as having direct experience conducting penetration testing (network, web application, and mobile application penetration testing). There is no mention of experience testing thick clients, mainframes, or ICS/SCADA within the resumes.
Qualifications Section Total Score	65.0	26.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	12.0	Bidder provides a sample reort of internal, external, and web application penetration testing (pg. 59). The report includes an executive summary and a summary of areas of opportunity, but does not provide a summary of areas of strength. The detailed findings include a "HydraRisk" score that breaks down the consequence, probability, velocity, criticality, and responsiveness of each finding. The findings contain a brief description, supporting evidence (screenshots), recommendations with varying levels of detail, and additional references.
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	38.0	
Evaluator Initials : JOC			
Date: 5/22/23			

K689 - Security Assessment Services			
Vendor: WWT			
Quotations Section Section - Cost Proposal (10%)			
Cost Proposal	Total Possible Points	Scoring	Notes
The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price. The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. We will include both the blended hourly rate and the price quote in scoring the cost proposal. <u>This is done by contract manager.</u>	10.0		Score will be calculated by contracts coordinator. Please add comments as you see fit.  JOC 5/22/23: Bidder's blended hourly rate (\$569) is <b>extremely</b> high, and is <b>over \$200/hour higher than the 2nd highest bidder</b> . The sample agency cost (\$264,585) is also extremely high, and not sustainable if SAO plans to audit the full amount of entities enumerated in the RFQQ.
Price Proposal Total Score	10.0	0.0	
Qualifications Section (65%)			
Experience/Staffing	Total Possible Points	Scoring	Notes
Experience (35%)	35.0	7.0	Bidder states they plan to use subcontractors for this work (Palo Alto Networks).  Bidder disclosing having provided non-audit services to a number of Washington state agencies and local governments (pgs. 13-14).  Bidder only provides two references as part of their proposal, stating they "can provide additional references upon down-select." <b>The RFQQ explicitly asked for three references.</b>  Beyond including language from the RFQQ, the <b>bidder's proposal does not mention experience testing on thick client applications, mainframes, or ICS/SCADA systems at all, and only provides an ambiguous reference to experience testing mobile applications in one of the resumes.</b>  Bidder provides case studies as representative examples (pgs. 63-82), however <b>none of them explicitly included penetration testing</b> , and only one (Project 1) had language that suggests that penetration testing <b>might</b> have been included in the scope of work (a "comprehensive security assessment"). Projects 1, 2, and 5 are incident response engagements, and Project 4 was an engagement focused on building/rebuilding a stronger and more mature security environment post-recovery. Although Project 3 did include Purple Team exercises, it was actually just a test of the customer's detection and response capabilities in accordance with the NIST Cybersecurity Framework (CSF), and was <b>not</b> a penetration test engagement with the purpose of identifying existing technical vulnerabilities in the customer's networks and applications. Furthermore, <b>none of the case studies mention experience conducting testing of any kind on web applications, thick clients, mainframes, ICS/SCADA systems, or mobile applications.</b>
Staffing (30%)	30.0	12.0	Bidder provides resumes for two individuals (pgs. 58-61), both of whom are listed as having extensive expereince conducting penetration tests. However, the resumes do not provide much detail in terms of the types of penetration testing the two individuals have conducted beyond network testing/red teaming, web application testing, and possibly mobile device testing (this is listed as a skill in the resume for Bill Barshbarger, but not articulated as something that the individual has conducted as part of an engagement). For example, they do not speciv if the individuals have conducted testing on mobile applications, thick clients, mainframes, or ICS/SCADA systems.
Qualifications Section Total Score	65.0	19.0	
Sample Report (15%)			
This sample report will be scored based on how well its components respond to items listed under item "d." under "Report Results" on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.	15.0	6.0	Bidder provided a sample penetration test report (pg. 96) for an external penetration test, including a website. The report includes an executive summary and a summary of recommendations (areas for improvement), <b>but does not include a summary of areas of strength</b> . The report's detailed findings are rated by impact and exploitability, and are supported with evidence (screenshots) and some additional references. <b>However, the descriptions and recommendations for the findings are very brief and do not include much context for the environment.</b>
Procurement Eval for Executive Order 18-03 & WA Small Business/Veteran Owned Business (10%)			
This will be scored and provide a bid preference in the way of 5 points to any bidder certifies, that their firm does NOT require its employees, as a condition of employment to sign or agree to mandatory individual arbitration clauses or class or collective action waiver and/or Washington Small Business/Certified Veteran Owned.	10.0		Score will be calculated by contracts coordinator.
Vendor's Total Score for Proposal (out of 100%)	100.0	25.0	
Evaluator Initials : JOC			
Date: 5/22/23			